



The Expanding Web of Cybersecurity Requirements

Patrick C Miller, President and CEO

May 11 2011

UTC TELECOM 2011

Abstract



“...security is an art – and you cannot legislate art.”

- Bill Bryan, Deputy Assistant Secretary of Infrastructure Security & Energy Restoration, US DOE

Levity, Sort Of



So there was this investor owned, self-insured utility with a critical generation plant in a maritime port with an onsite credit union and urgent care facility who processed their own credit card transactions... (PCI, SOX, GLBA, MTSA, HIPAA, NERC CIP, CFATS, state PII)

...and the transmission bus was in an adjacent facility owned by a Federal Power Marketing Authority... (add FISMA)

Cybersecurity Landscape



- Security regulations favor new installations, legacy environments are still vulnerable
 - Bolt-ons increase complexity
 - Mixing legacy and bleeding edge tech is difficult
- Isolation has diminishing security value
- Engineering and Security are different
- Logical distance between kinetic endpoint and HMI is exponentially increasing; “hyperembeddedness”
- Nation-state quality defense is the new norm

Smart Grid Standards



- FERC/NERC/PUC lines are not clear
- Some state commissions do not have expertise or sufficient staff to deal with the smart grid wave
- Commissions and utilities are both moving forward, but inconsistently
- Privacy and security will be significant issues
- Suffering from standard fatigue

NERC CIP Standards



The Bad News:

- Often viewed as ceiling vs. floor
- Little change in over a decade
- Technical Feasibility Exceptions

The Good News:

- Formalized security as a real issue within industry
- Known minimum bar
- Fantastic growth potential

Future Standards?



- Cyber-boogeyman, cyber-FUD
- Who's got the cyber legislation pole position?
- Threats move faster than legislation and regulation
- Hackers don't use a checklist
- If you want legislation really bad, you will get really bad legislation; same for regulation
 - Converse = analysis paralysis; seek equilibrium
- Good security wasn't invented yesterday

Future Standards?



- Intelligent islanding?
- Data breach disclosure?
- Vendor/product responsibility?
- Utility responsibility?
- Federal presence?
- Does self-regulation work?
- Top down or bottom up – or both?

The Question



- Long: How do we get simple, complementary and comprehensive cyber legislation for all interdependent critical infrastructures, based on solid actuarial risk data, to protect both the public and private sectors but doesn't cause rates/costs to rise to unacceptable levels?
- Short: Fast, inexpensive, good. Pick two.

Questions?



Non-profit. Independent. Trusted.



Patrick C Miller, President and CEO
patrick@energysec.org
503-446-1212

*The National Electric Sector Cybersecurity Organization
(NESCO) is a DOE-funded EnergySec Program*